

*Л. Д. Какабаева*¹✉

Метод централизованного управления сетевым оборудованием и средствами обеспечения сетевой безопасности

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: leyli.kakabayeva@bk.ru

Аннотация. В статье рассматривается задача централизованного управления сетевым оборудованием и средствами обеспечения сетевой безопасности в корпоративных вычислительных сетях. Актуальность исследования обусловлена ростом числа атак через эксплуатацию уязвимостей сетевого оборудования, требованиями нормативно-правовых актов Российской Федерации, а также возникновением большого количества ошибок при ручном децентрализованном конфигурировании. Цель исследования заключается в обеспечении аутентичности объектов сетевой инфраструктуры предприятия и подотчетности действий ее пользователей посредством централизованного управления. В работе предложен метод, основанный на криптографической аутентификации операций с использованием алгоритма Ed25519, управлении доступом на основе capability-токенов, программной аттестации устройств и обеспечении целостности журналов аудита на основе цепочки хеш-значений. Разработан четырехфазный протокол развертывания конфигураций, обеспечивающий атомарность изменений и возможность отката. Программная реализация системы (ZT-NMS) прошла комплексное тестирование, продемонстрировавшее достижение целевых показателей производительности и устойчивость к основным типам атак. Сравнительный анализ с существующими решениями подтвердил преимущества предложенного метода в части обеспечения механизмов безопасности.

Ключевые слова: централизованное управление, сетевое оборудование, средства защиты информации, capability-токены, аттестация устройств, журналы аудита

*L. D. Kakabaeva*¹✉

Method for centralized management of network equipment and network security tools

¹National Research Nuclear University MEPhI, Moscow, Russian Federation
e-mail: leyli.kakabayeva@bk.ru

Abstract. The article addresses the task of centralized management of network equipment and network security tools in corporate computing networks. The relevance of the research is due to the growing number of attacks exploiting vulnerabilities in network equipment, the requirements of regulatory acts of the Russian Federation, as well as a large number of errors in manual decentralized configuration. The aim of the study is to ensure the authenticity of network infrastructure assets of an enterprise and the accountability of user actions through centralized management. The paper proposes a method based on cryptographic authentication of operations using the Ed25519 algorithm, capability-based access control, software attestation of devices, and integrity protection of audit logs based on a hash chain. A four-phase configuration deployment protocol is designed to ensure atomicity of changes and rollback capability. The software implementation of the system (ZT-NMS) underwent comprehensive testing, demonstrating the achievement of target performance metrics and resilience to main types of attacks. A comparative analysis with existing solutions confirmed the advantages of the proposed method in terms of security mechanisms.

Keywords: centralized management, network equipment, network security tools, capability tokens, device attestation, audit logs

Введение

Информационная безопасность сетевой инфраструктуры предприятия определяется не только корректностью настройки отдельных средств защиты информации (СЗИ), но и согласованностью конфигураций всего парка сетевого оборудования. Согласно отчету Verizon Data Breach Investigations Report 2025, эксплуатация уязвимостей сетевого оборудования стала одним из основных векторов атак на корпоративные сети [1]. При этом значительная часть инцидентов связана не с уязвимостями нулевого дня, а с ошибками конфигурации, возникающими при ручном децентрализованном администрировании.

Актуальность темы исследования подтверждается требованиями нормативно-правовых актов Российской Федерации. Указ Президента РФ от 1 мая 2022 г. № 250 устанавливает дополнительные меры по обеспечению информационной безопасности, включая обязательный переход на отечественные СЗИ [2]. Постановление Правительства РФ от 12 февраля 2020 г. № 127 утверждает «Правила централизованного управления сетью связи общего пользования» [3]. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 рекомендует применять централизованное управление подсистемой безопасности значимого объекта.

В научной среде задача централизованного управления сетевым оборудованием рассматривается в работах нескольких исследовательских групп. Архитектурная методология SDN с разделением плоскостей управления и данных через стандартизированный интерфейс OpenFlow развивается в работах N. McKeown, S. Shenker и J. Rexford [4]. Метод автоматического распределения и конфигурирования пакетных фильтров в сервисном графе предложен D. Brighenti, R. Sisto и F. Valenza [5]. Архитектурно-ориентированная методология проектирования SOAR-платформы рассматривается в работах С. Islam [6]. Методология построения типового центра интеллектуального управления сетевой безопасностью разработана Н. Г. Милославской [7]. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предложена Е. А. Басыней [8–10].

Несмотря на значительный объем проведенных исследований, в существующих работах не сформирован единый теоретико-методологический аппарат, охватывающий централизованное управление гетерогенным сетевым оборудованием и СЗИ в рамках одного жизненного цикла. Не разработана формальная модель взаимодействия контроллера с гетерогенными СЗИ, отсутствует теория абстракции функций безопасности для Northbound API. Анализ существующих коммерческих и открытых решений (NOC Project, rConfig, HPE IMC, Eltex.EMS, QNAP QRM+, TP-Link tpNMS, HOTA Купол) показал, что ни одно из них не реализует одновременно все ключевые механизмы обеспечения безопасности: криптографическую аутентификацию операций, использование токенов доступа, аттестацию устройств и контроль целостности журналов аудита [11].

Цель исследования заключается в обеспечении аутентичности объектов сетевой инфраструктуры предприятия и подотчетности действий ее пользователей посредством централизованного управления СЗИ и сетевым оборудованием. Для достижения цели поставлены задачи: исследование предметной области; моделирование объектов и процессов; разработка и программная реализация системы централизованного управления; тестирование и сравнительный анализ предложенного решения с существующими.

Методы и материалы

Предлагаемый метод централизованного управления сетевым оборудованием и средствами обеспечения сетевой безопасности базируется на четырех основных механизмах: криптографической аутентификации операций с использованием алгоритма Ed25519 [12], управлении доступом на основе capability-токенов, программной аттестации управляемых устройств и обеспечении целостности журналов аудита на основе цепочки хеш-значений.

Архитектура системы построена по принципу разделения на слои и реализована в виде набора слабосвязанных компонентов. В состав плоскости управления входят: сервис идентификации (Identity Service), отвечающий за управление учетными записями и аутентификацию субъектов; модуль выпуска capability-токенов (Capability Issuer), обеспечивающий генерацию и подписание токенов доступа; менеджер конфигураций (Config Manager); верификатор аттестации (Attestation Verifier); сервис аудита (Audit Service); прокси-компонент устройств (Device Proxy). Внешний доступ к системе осуществляется через API-шлюз с применением транспортного протокола TLS версии 1.3. Архитектура системы централизованного управления приведена на рис. 1.

Аутентификация операторов реализована по схеме challenge-response на основе эллиптической криптографии. Клиентское приложение генерирует ключевую пару Ed25519, после чего публичный ключ регистрируется в сервисе идентификации. При аутентификации сервер выдает случайное значение (challenge), которое подписывается приватным ключом оператора и проверяется сервером с использованием зарегистрированного публичного ключа. При успешной верификации формируется токен доступа.

Управление доступом реализовано на основе модели capability-based access control. Capability-токен содержит идентификатор субъекта, список грантов (ресурс, действия, ограничения), правила делегирования, период действия и подпись издателя. Перед выпуском токена движок политик (Policy Engine) оценивает запрос на основе атрибутов субъекта, ресурса и контекста. Защита от атак воспроизведения обеспечивается хранилищем одноразовых случайных значений (NonceStore).

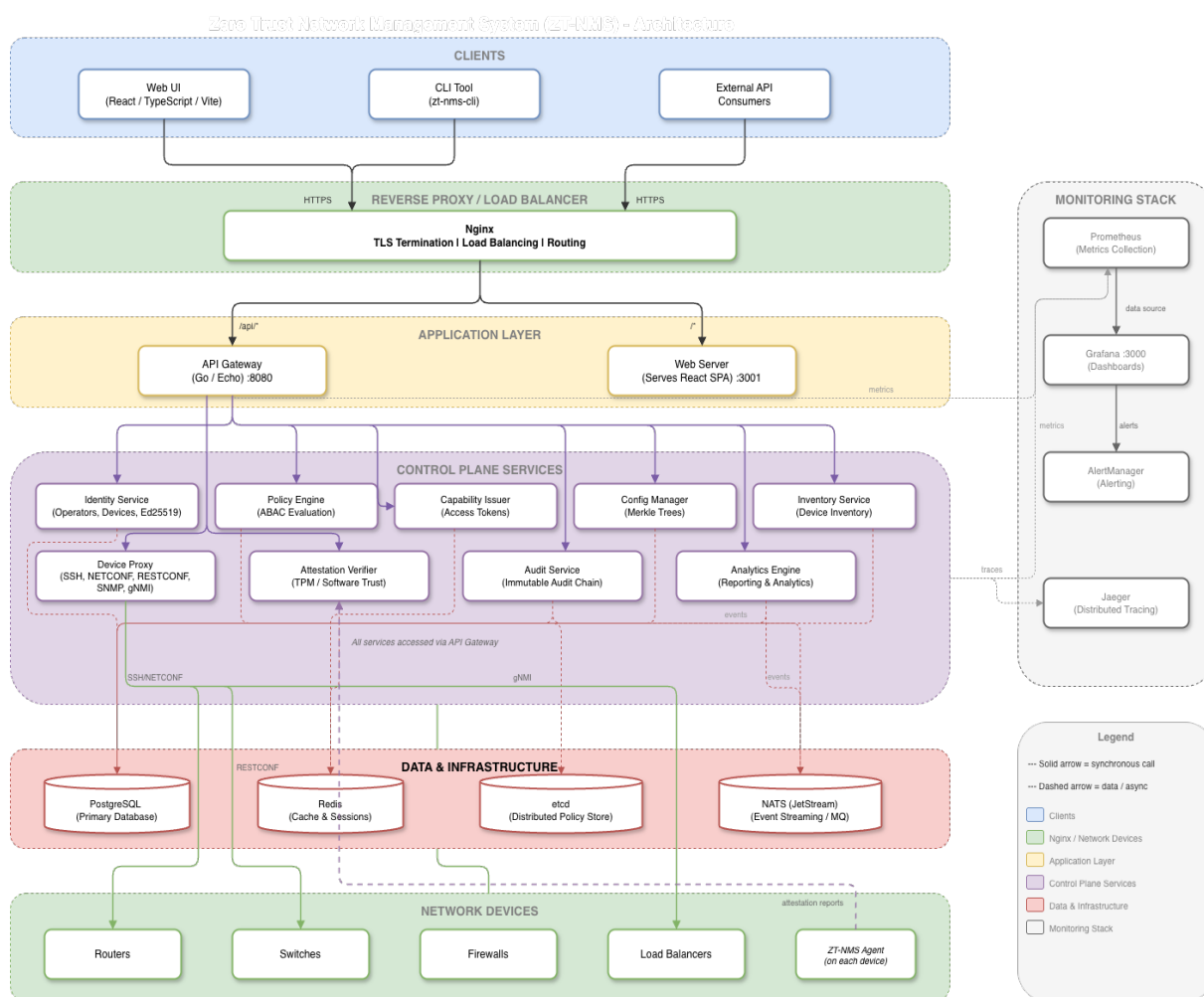


Рис. 1. Архитектура системы централизованного управления

Логика функционирования системы централизованного управления, реализующая описанные механизмы, представлена на рис. 2 в виде блок-схемы. Развертывание конфигураций на управляемые устройства осуществляется по разработанному четырехфазному протоколу, обеспечивающему атомарность изменений и возможность отката. Фаза *validating* включает проверку синтаксиса конфигурации, валидацию относительно действующих политик безопасности и проверку отсутствия потенциально опасных конструкций. На фазе *preparing* система формирует структуру *ConfigBlock*, содержащую предлагаемую конфигурацию, ее хеш-значение и хеш-значение предыдущего блока, образуя непрерывную цепочку. На фазе *committing* команда фиксации передается на устройство, где агент применяет подготовленную конфигурацию. Фаза *verifying* включает запрос текущей конфигурации с устройства, вычисление ее хеш-значения и сравнение с ожидаемым значением; при несовпадении инициируется автоматический откат.

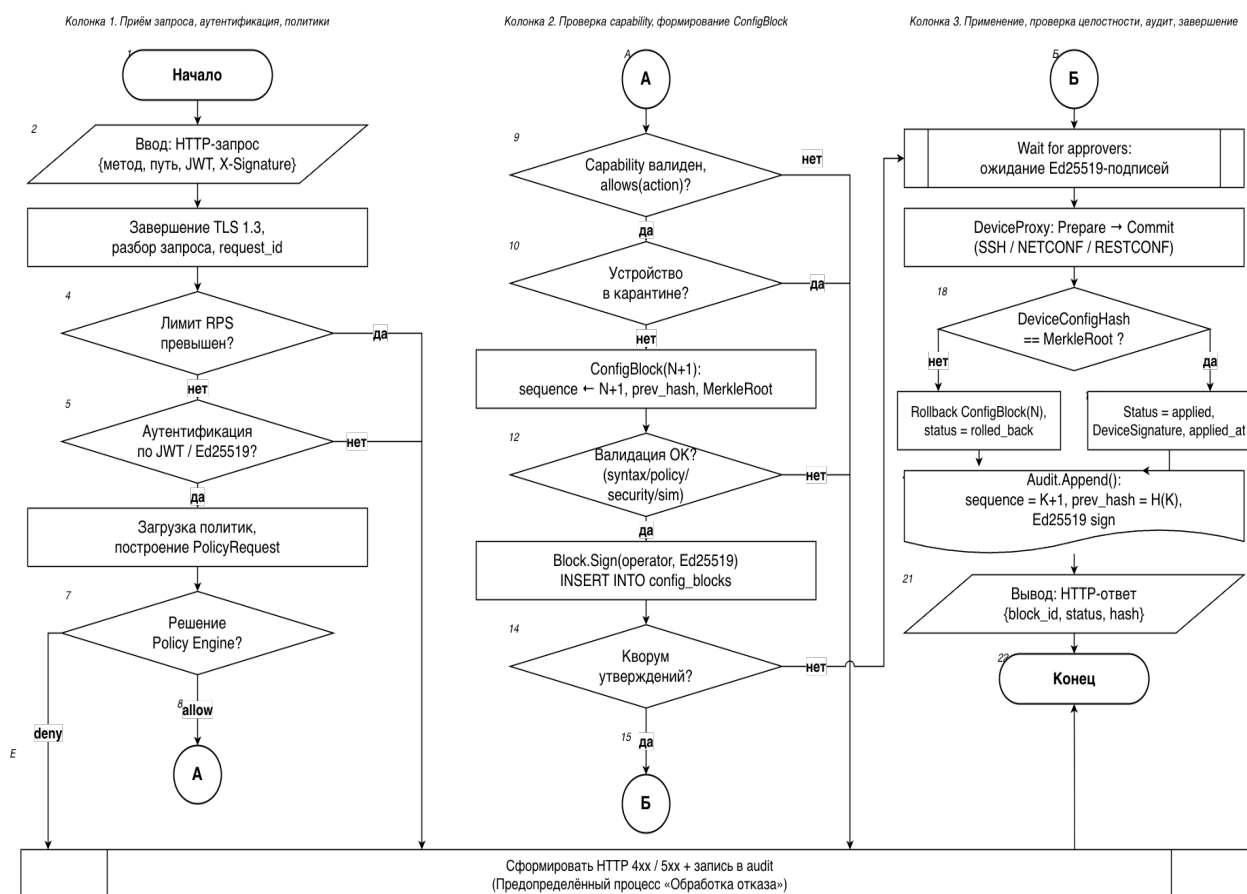


Рис. 2. Блок-схема работы системы централизованного управления

Программная аттестация управляемых устройств обеспечивает контроль целостности их программного обеспечения. Агент на устройстве собирает набор измерений (хеш-значения встроенного ПО, операционной системы, конфигурации и исполняемого файла агента), объединяет их с одноразовым значением, полученным от сервера, и подписывает результат своим приватным ключом. Сервис верификации сравнивает полученные измерения с эталонными значениями и обновляет статус доверия устройства.

Журналирование событий безопасности реализовано на основе цепочки хеш-значений. Каждое событие аудита содержит хеш-значение предыдущего события, обеспечивая возможность последующей верификации целостности журнала. Любая модификация или удаление событий приводит к нарушению цепочки и обнаруживается при верификации.

Результаты

На основе предложенного метода реализована программная система централизованного управления ZT-NMS. Для разработки выбран язык Go версии 1.22 в сочетании с фреймворком Echo v4, обеспечивающим высокую пропускную способность HTTP-обработчиков. В качестве хранилища используется PostgreSQL 16 с расширением pgvector, кеширование решений политик и хранение nonce

реализовано на Redis 7, шинная интеграция событий обеспечивается NATS JetStream. Контейнеризация и оркестрация выполняются на базе Kubernetes 1.29.

Для проверки корректности и производительности системы разработана технологическая дорожная карта тестирования, включающая шесть фаз: модульное, интеграционное, системное тестирование, тестирование безопасности, нагрузочное и приемочное тестирование. Проведено 348 модульных тестов с покрытием исходного кода 88 %, что превышает целевое значение в 80 %. Все 20 интеграционных тестов и 20 тестов безопасности успешно пройдены. Нагрузочное тестирование подтвердило достижение целевых показателей производительности: время верификации подписи Ed25519 – 0,09 мс при целевом значении менее 0,1 мс; время выпуска sarability-токена – 12 мс при целевом значении менее 50 мс; пропускная способность API-шлюза – 2340 запросов в секунду при целевом значении более 1000; время записи события в журнал аудита – 3 мс при целевом значении менее 10 мс.

Сравнение функциональных возможностей предложенной системы ZT-NMS с распространенными решениями (NOC Project, rConfig) показало, что разработанная система обладает наиболее полным набором механизмов безопасности: реализованы криптографическая аутентификация операций, использование токенов доступа, аттестация устройств и контроль целостности журналов, отсутствующие в обеих сравниваемых системах. По функциональным возможностям все три системы обеспечивают базовый набор функций управления гетерогенными системами, резервного копирования и развертывания конфигураций.

По показателю времени первичной аутентификации система ZT-NMS демонстрирует наилучший результат среди сравниваемых решений (150 мс против 185 мс у NOC Project и 320 мс у rConfig), что объясняется применением алгоритма Ed25519 и кешированием результатов проверки политик. Время применения изменений и отката увеличено относительно NOC Project, что обусловлено выполнением четырехфазного протокола развертывания и формированием криптографических подписей; данное увеличение является приемлемой платой за обеспечение целостности и подотчетности изменений.

Обсуждение

В отличие от существующих решений централизованного управления, ориентированных преимущественно на удобство администрирования, предложенный метод изначально проектировался с учетом требований обеспечения аутентичности и подотчетности. Криптографическая привязка операций к идентичности оператора через подпись Ed25519 исключает возможность отказа от авторства совершенного действия. Использование sarability-токенов с явным перечнем грантов обеспечивает выполнение принципа минимальных привилегий: токен может предоставлять доступ только к конкретному набору устройств и действий и имеет ограниченный срок действия [13].

Четырехфазный протокол развертывания конфигураций обеспечивает гарантии атомарности и возможность автоматического отката, что особенно важно при массовом обновлении гетерогенного парка сетевого оборудования. Цепочка

хеш-значений в журнале аудита обеспечивает обнаружение модификаций журнала, что исключает возможность скрытия следов атаки путем подделки записей [14].

Ограничениями предложенного метода являются увеличение времени отдельных операций по сравнению с системами, не использующими криптографические механизмы, и необходимость наличия агента на управляемых устройствах для выполнения процедуры аттестации. Для устройств без возможности установки агента предусмотрен режим работы с ограниченной функциональностью без проведения программной аттестации.

Заключение

В ходе исследования рассмотрена задача централизованного управления сетевым оборудованием и средствами обеспечения сетевой безопасности в корпоративных вычислительных сетях. Предложен метод централизованного управления, основанный на криптографической аутентификации операций, capability-токенах, программной аттестации устройств и обеспечении целостности журналов аудита.

Разработана и программно реализована система централизованного управления ZT-NMS. Проведено комплексное тестирование, подтвердившее корректность функционирования и достижение целевых показателей производительности. Сравнительный анализ с существующими решениями (NOC Project, rConfig) подтвердил преимущества предложенного метода в части обеспечения механизмов безопасности [15].

В дальнейшем планируется расширение поддержки сетевого оборудования и СЗИ различных вендоров, интеграция с системами анализа инцидентов и реагирования на угрозы, а также развитие математического аппарата унифицированного управления политиками для гетерогенных СЗИ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Verizon Business. 2025 Data Breach Investigations Report. – Verizon, 2025. – URL: <https://www.verizon.com/business/resources/reports/dbir/> (дата обращения: 04.05.2026).
2. Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». – URL: <http://publication.pravo.gov.ru/Document/View/0001202205010023> (дата обращения: 27.12.2025).
3. Постановление Правительства РФ от 12 февраля 2020 г. № 127 «Об утверждении Правил централизованного управления сетью связи общего пользования». – URL: <https://base.garant.ru/73567870/> (дата обращения: 27.12.2025).
4. McKeown N., Anderson T., Balakrishnan H. et al. OpenFlow: Enabling Innovation in Campus Networks // ACM SIGCOMM Computer Communication Review. – 2008. – Т. 38, № 2. – С. 69–74.
5. Bringhenti D., Sisto R., Valenza F., Marchetto G. Automation for Network Security Configuration: State of the Art and Research Trends // ACM Computing Surveys. – 2025. – Т. 56, № 3.
6. Islam C., Babar M.A., Nepal S. Architecture-Centric Support for Integrating Security Tools in a Security Orchestration Platform // Proc. of European Conference on Software Architecture (ECSA 2020). – 2020.

7. Милославская Н.Г., Толстой А.И. Управление информационной безопасностью: учебное пособие. – М.: НИЯУ МИФИ, 2020. – 256 с.
8. Басыня Е.А. Сетевая информационная безопасность: учебник. – М.: НИЯУ МИФИ, 2023. – 224 с.
9. Басыня Е.А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия // Защита информации. Инсайд. – 2021. – № 5 (101). – С. 16–25.
10. Басыня Е.А., Худяков Д.С. Комплексный мониторинг информационной инфраструктуры предприятия // Защита информации. Инсайд. – 2020. – № 6 (96). – С. 28–33.
11. NOC Project: официальный сайт. – URL: <https://getnoc.com/> (дата обращения: 09.01.2026).
12. Bernstein D.J., Duif N., Lange T., Schwabe P., Yang B.-Y. High-speed high-security signatures // Journal of Cryptographic Engineering. – 2012. – Т. 2, № 2. – С. 77–89.
13. Зегжда Д.П., Калинин М.О., Полтавцева М.А. Методы защиты сетевой инфраструктуры в программно-определяемых сетях // Труды СПбГЭТУ «ЛЭТИ». – 2021.
14. Kreutz D., Ramos F.M.V., Verissimo P.E. et al. Software-Defined Networking: A Comprehensive Survey // Proceedings of the IEEE. – 2015. – Т. 103, № 1. – С. 14–76.
15. Siddiqui A., Rimal B.P. Unified Threat Management Framework for Home Networks // Dakota State University Scholar. – 2024.

© Л. Д. Какабаева, 2026